Roll No. ....

E–1063

M. Sc. (IT) (Fourth Semester)

EXAMINATION, May-June, 2021

(New Course)

CYBER SECURITY

M. Sc. (IT) (401)

Time : Three Hours]　　　　　　[*Maximum Marks : 100*

　　　　　　　　　　　　　[*Minimum Pass Marks : 40*

Note : Attempt all Sections as directed.

Section—A　　　　1 each

(Objective/Multiple Choice Questions)

Note : Attempt all questions.

Choose the correct answer :

1. Which one of the following can be considered as the class of computer threats ?

    (a) DOS Attack

    (b) Phishing

    (c) Soliciting

    (d) Both (a) and (c)

P. T. O.

2. Which of the following is considered as the unsolicited commericial email ?

    (a) Virus

    (b) Malware

    (c) Spam

    (d) All of the above

3. Which of the following usually observe each activity on the internet of the victim, gather all information in the background and send it to someone else ?

    (a) Malware

    (b) Spyware

    (c) Adware

    (d) All of the above

4. .... is a type of software designed to help the user's computer detect viruses and avoid them.

    (a) Malware

    (b) Adware

    (c) Antivirus

    (d) Both (b) and (c)

5. Which of the following types of text is transformed with the help of a cipher algorithm ?

    (a) Transformed text

    (b) Complex text

    (c) Scalar text

    (d) Plain text

6. Public key cryptography is also known as :

   (a)   asymmetric cryptography

   (b)   symmetric cryptography

   (c)   Both (a) and (b)

   (d)   None of the above

7. Examples of hash function are :

   (a)   MD5

   (b)   SHA-1

   (c)   Both (a) and (b)

   (d)   None of the above

8. Private key algorithm is used for .... encryption and public key algorithm is used for .... encryption.

   (a)   messages, session key

   (b)   session key, messages

   (c)   Can be used for both

   (d)   None of the above

9. In public key cryptosystem which is kept as public ?

   (a)   Decryption keys

   (b)   Encryption keys

   (c)   Encryption and Decryption keys

   (d)   None of the above

P. T. O.

10. In public key cryptosystem .... keys are used for encryption and decryption.

    (a)   Same

    (b)   Different

    (c)   Encryption

    (d)   None of the mentioned

11. Another name for message authentication codes is ....

    (a)   Cryptographic codebreak

    (b)   Cryptographic codesum

    (c)   Cryptographic checksum

    (d)   Cryptographic checkbreak

12. MACs are also called :

    (a)   testword

    (b)   checkword

    (c)   test bits

    (d)   None of the mentioned

13. Message authentication is a service beyond :

    (a)   Message confidentiality

    (b)   Message integrity

    (c)   Message splashing

    (d)   Message sending

14. A digital signature needs a :

(a) Private-key system

(b) Shared-key system

(c) Public-key system

(d) All of the above

15. Which of the following are objectives of malware ?

(a) Provide remote control for an attacker to use an infected machine

(b) Investigate the infected user's local network

(c) Steal sensitive data

(d) All of the above

16. Which of the following malware do not replicate or reproduce through infection ?

(a) Worms

(b) Trojans

(c) Viruses

(d) Root kits

17. Firewalls can be of .... kind(s).

(a) 1

(b) 2

(c) 3

(d) 4

P. T. O.

18. .... is the kind of firewall connected between the device and the network connecting to internet.

(a) Hardware firewall

(b) Software firewall

(c) Stateful inspection firewall

(d) Microsoft firewall

19. .... is a tool which can detect registry issues in an operating system.

(a) Network stumbler

(b) Etter cap

(c) Maltego

(d) Languard network security scanner

20. Firewall examines each .... that are entering or leaving the internal network.

(a) email users

(b) updates

(c) connections

(d) data packets

Section—B 2 each

(Very Short Answer Type Questions)

Note : Attempt all questions. Answer using 2-3 sentences.

1. What is cryptography ?

2. What is security attacks ?

3. What is public key cryptography ?

4. What is RSA ?

5. What is message integrity ?
6. What is digital signature ?
7. What is DDOS attack ?
8. Explain Nature of viruses.
9. What is Firewall ?
10. What is Kali Linux ?

Section—C   3 each
(Short Answer Type Questions)

Note : Attempt all questions. Answer pricisely using < 75 words.

1. What are Random and Pseudorandom Numbers ?
2. Explain challenges of computer security.
3. What are symmetric and asymmetric key systems ?
4. What is the hashing function ?
5. What is attacks of digital signature ?
6. What is message authentication code ?
7. What are the uses of usage of malware ?
8. What is Trojan Horse ? Give few examples.
9. What can a firewall protect IT infrastructure inside your organization ?
10. What is cyber security policy ?

Section—D   6 each
(Long Answer Type Questions)

Note : Attempt all questions. Answer precisely using 150 words.

1. What is Symmetric block modes of operation ? Also explain ECB, CBC, CFB and CTR.

Or

What do you mean by Security Services ? Explain benefits of cryptography and few major applications of cryptography in the modern world.

P. T. O.

2. What is the role of Hash function in message integrity ? Explain the criteria of random oracle model.

Or

What is RSA algorithm ? Explain attacks on RSA and OAEP.

3. What do you understand by message authentication ? Explain types of approaches to use for message authentication (any *one* approach).

Or

Explain the following :

(a) HMAC and CMAC

(b) Document and fingerprinting

(c) Process services

4. What is the difference between statical intrusion detection and distributed intrusion selection.

Or

Write on short notes on the following :

(a) Virus and their types

(b) Antivirus approaches

(c) Worm and its propagation model

5. What is firewall basing ? Write the characteristics of firewall and their types.

Or

Explain the tools available in Kali Linux and its usage (briefly explain).

E–1063   **200**